

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-138969

(43)Date of publication of application : 20.05.1994

(51)Int.Cl.

G06F 1/00
G06F 15/00

(21)Application number : 04-288399

(71)Applicant : HITACHI LTD

(22)Date of filing : 27.10.1992

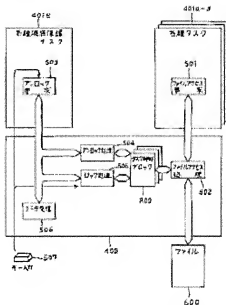
(72)Inventor : KUWAMOTO HIDEKI
IWATANI TAKAO
OZAKI TOMOYA

(54) SECURITY SYSTEM

(57)Abstract:

PURPOSE: To prevent the illegal use of a file by setting a security state anytime when a user wants it.

CONSTITUTION: When various tasks 401 make an access to a file 600, a file access processing 502 called by a file access processing request 501 collates a user ID of the file 600 with the user ID of a task control block 800, limiting the access of the file 600 by the task 401 according to the file protection attribute of the file 600. An unlock processing 504 is called by an unlock request 503 of various security tasks 401e called by the direction of a user by key input 507 or the like and data reception 506 which directs unlocking, setting the user ID of the task control block 800. Thus, the illegal use of the file can be prevented.



【特許請求の範囲】

【請求項1】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第1の情報処理装置と、その情報装置が設置されている部屋の入室退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第2の情報処理装置からなる情報処理システムにおいて、

該情報処理装置の利用者が該部屋への入室の通知を該第2の情報処理装置に入力する入力手段と、
該第2の情報処理装置が、該利用者の該部屋への入室の通知を入力されたならば、該利用者を識別する利用者識別子と入室であることを記した入室データを第1の情報処理装置に通知する入室データ送信手段と、
該第1の情報処理装置が該入室データを受信したならば、利用者の区別によって読書きが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスを、直ちに可能にする機密保護解除手段を有することを特徴とする機密保護方式。

【請求項2】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第1の情報処理装置と、その情報装置が設置されている部屋の入室退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第2の情報処理装置からなるシステムにおいて、
該情報処理装置の利用者が該部屋からの退室の通知を該第2の情報処理装置に入力する入力手段と、
該第2の情報処理装置が、該利用者の該部屋からの退室の通知を入力されたならば、該利用者を識別する利用者識別子と退室であることを記した退室データを第1の情報処理装置に通知する退室データ送信手段と、
該第1の情報処理装置が該退室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスを、直ちに解除する機密保護設定手段を有することを特徴とする機密保護方式。

【請求項3】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第1の情報処理装置と、その情報装置が設置されている部屋の入室退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第2の情報処理装置からなるシステムにおいて、
該情報処理装置の利用者が該部屋への入室の通知を該第2の情報処理装置に入力する入力手段と、
該第2の情報処理装置が、該利用者の該部屋への入室の通知を入力されたならば、該利用者を識別する利用者識別子と入室であることを記した入室データを第1の情報処理装置に通知する入室データ送信手段と、
該情報処理装置で動作するタスクに、該タスクの起動を依頼した利用者を示す利用者識別子に対応づける手段と、

該第1の情報処理装置が該入室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスが可能な状態を、該利用者識別子と同一の利用者識別子に対応づけられているタスクに直ちに設定する機密保護解除手段を有することを特徴とする機密保護方式。

【請求項4】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第1の情報処理装置と、その情報装置が設置されている部屋の入室退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第2の情報処理装置からなるシステムにおいて、
該情報処理装置の利用者が該部屋からの退室の通知を該第2の情報処理装置に入力する入力手段と、
該情報処理装置で動作するタスクに、該タスクの起動を依頼した利用者を示す利用者識別子に対応づける手段と、

該第2の情報処理装置が、該利用者の該部屋からの退室の通知を入力されたならば、該利用者を識別する利用者識別子と退室であることを記した退室データを第1の情報処理装置に通知する退室データ送信手段と、
該第1の情報処理装置が該退室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子で示される利用者にのみ許されるアクセスが不可能な状態を、該利用者識別子と同一の利用者識別子に対応づけられているタスクに直ちに設定する機密保護設定手段を有することを特徴とする機密保護方式。

【請求項5】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第1の情報処理装置と、その情報装置が設置されている部屋の入室退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第2の情報処理装置からなるシステムにおいて、
第1の情報処理装置に、
データの特定の利用者を識別する利用者識別子と、特定の利用者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータと、
実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子を格納したタスク制御ブロックと、
利用者識別子と暗証番号の対応関係を記述した暗証番号管理テーブルと、
利用者が、他人へのアクセスを禁止したデータをアクセスするために、利用者識別子と暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除を該情報処理装置に指示する第1の入力手段と、
利用者が、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすることを禁止する状態にするために、第1の入力手段を用いた指示により解除された機密保護状態を解除前の状態に戻す、つまり、機密保

3

護状態を設定する指示を行う第2の入力手段と、
第1の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係を、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに、指定された利用者識別子を記述する第1の制御手段と、
タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子とアクセスを行うタスクに対応するタスク制御ブロックの利用者識別子が一致する
10 かどうかを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第2の制御手段と、

第2の入力手段により機密保護状態の設定の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第3の制御手段と、
入室を管理する第2の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第4の制御手段と、
入室を管理する第2の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに該利用者識別子を格納する第5の制御手段とを設け、

第2の情報処理装置に、
入室する利用者の利用者識別子を入力する第1の入力手段と、
退室する利用者の利用者識別子を入力する第2の入力手段と、
入室する利用者の利用者識別子が第1の入力手段により入力されたならば、該利用者識別子の利用者識別子を入室した利用者の利用者識別子として、第1の情報処理装置に通知する第1の制御手段と、
退室する利用者の利用者識別子が第2の入力手段により入力されたならば、該利用者の利用者識別子を退室した利用者の利用者識別子として、第1の情報処理装置に通知する第2の制御手段とを設けたことを特徴とする機密保護方式。

【請求項6】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第1の情報処理装置と、その情報装置が設置されている部屋の入室を管理するため、中央処理装置と記憶装置と入力装置と通信装置から

4

なる第2の情報処理装置からなるシステムにおいて、
第1の情報処理装置に、
データの特定の利用者を識別する利用者識別子と、特定の利用者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータと、
実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子を格納したタスク制御ブロックと、

利用者識別子と暗証番号の対応関係を記述した暗証番号管理テーブルと、
利用者が、他人へのアクセスを禁止したデータをアクセスするために、利用者識別子と暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除を該情報処理装置に指示する第1の入力手段と、

第1の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係を、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに、指定された利用者識別子を記述する第1の制御手段と、
タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子とアクセスを行うタスクに対応するタスク制御ブロックの利用者識別子が一致するかどうかを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第2の制御手段と、

入室を管理する第2の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに該利用者識別子を格納する第4の制御手段とを設け、

第2の情報処理装置に、
入室する利用者の利用者識別子を入力する第1の入力手段と、
入室する利用者の利用者識別子が第1の入力手段により入力されたならば、該利用者の利用者識別子を入室した利用者の利用者識別子として、第1の情報処理装置に通知する第1の制御手段とを設けたことを特徴とする機密保護方式。

【請求項7】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第1の情報処理装置と、その情報装置が設置されている部屋の入室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第2の情報処理装置からなるシステムにおいて、
第1の情報処理装置に、

データの特定の利用者を識別する利用者識別子と、特定

5

の利用者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータと、実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子を格納したタスク制御ブロックと、

利用者識別子と暗証番号の対応関係を記述した暗証番号管理テーブルと、

利用者が、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすることを禁止する状態にするために、第1の入力手段を用いた指示により解除され

た機密保護状態を解除前の状態に戻す、つまり、機密保護状態を設定する指示を行う第2の入力手段と、

タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子とアクセスを行うタスクに対応するタスク制御ブロックの利用者識別子が一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者

以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが許可の場合は該データをアクセスする

処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第1の制御手段と、

第2の入力手段により機密保護状態の設定の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第3の制御手段と、

入室を管理する第2の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第5の制御手段と、

第2の情報処理装置に、退室する利用者の利用者識別子を入力する第2の入力手段と、

退室する利用者の利用者識別子が第2の入力手段により入力されたならば、該利用者の利用者識別子を退室した利用者の利用者識別子として、第1の情報処理装置に通知する第2の制御手段とを設けたことを特徴とする機密保護方式。

【請求項8】請求項2又は4記載の機密保護方式において、

該第1の情報処理装置が該退室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して、該退室データの利用者識別子で示される利用者に許されるアクセスが可能な状態を、オープン中のファイルがクローズした時点で直ちに解除する機密保護設定手段を有することを特徴とする機密保護方式。

【請求項9】請求項5又は7記載の機密保護方式におい

6

て、実行中の各タスクに対応して設け、該タスクの利用者を唯一に識別する利用者識別子を格納したタスク制御準備ブロックを設け、

第4の制御手段の代わりに、入室を管理する第2の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御準備ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第4Aの制御手段を設け、

オープン中のファイルがクローズした時点で、該ファイルをオープンしていたタスクに対応するタスク制御準備ブロックの利用者識別子を、該タスクに対応するタスク制御ブロックに直ちに格納する第4Bの制御手段を設けたことを特徴とする機密保護方式。

【請求項10】請求項1又は3記載の機密保護方式において、

利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスが可能な状態を該利用者識別子と同一の利用者識別子が対応づけられているタスクに設定する際は、その時点で既に該タスクに設定されている特定の利用者がアクセスが可能な状態を保持しながら、追記して設定することを特徴とする機密保護方式。

【請求項11】請求項10記載の機密保護方式において、

利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスが不可能な状態を該利用者識別子と同一の利用者識別子が対応づけられているタスクに設定する際は、該利用者に対してのみ該不可能な状態を該タスクに設定することを特徴とする機密保護方式。

【請求項12】請求項5又は6記載の機密保護方式において、タスク制御ブロックは、該タスクの利用者を識別する利用者識別子を複数格納可能とし、

第1の制御手段は、第1の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、タスク制御ブロックの利用者識別子フィールドに、その時点で既に該タスク制御ブロックの該利用者識別子フィールドに設定されている利用者識別子を保持しながら、追記して指定された利用者識別子を格納し、

第4の制御手段は、入室を管理する第2の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、タスク制御ブロックの利用者識別子フィールド

7

に、その時点で既に該タスク制御ブロックの該利用者識別子フィールドに設定されている利用者識別子を保持しながら、追記して指定された利用者識別子を格納することを特徴とする機密保護方式。

【請求項13】請求項5又は7記載の機密保護方式において、

第2の入力手段は、機密保護状態に戻したい利用者の利用者識別子とともに、入力し、

第3の制御手段は、第2の入力手段により機密保護状態の設定が、利用者識別子とともに指示されたときに、指定された利用者識別子と同一の利用者識別子が格納されているタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）し、

第5の制御手段は、入室室を管理する第2の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、タスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）することを特徴とする機密保護方式。

【請求項14】請求項4、4、5、7、8又は9記載の機密保護方式において、タスク制御ブロックまたはタスク制御準備ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する制御は、予め定められている画面を出力装置に表示することによって起動する手段を設けたことを特徴とする機密保護方式。

【請求項15】請求項14記載の機密保護方式において、タスク制御ブロックまたはタスク制御準備ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する制御は、予め定められている画面を予め定められている一定時間出力装置に表示した後に起動する手段を設けたことを特徴とする機密保護方式。

【請求項16】請求項2、4、5、7、8又は9記載の機密保護方式において、タスク制御ブロックまたはタスク制御準備ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する制御は、予め定められている入力装置からの入力において、無入力の時間が予め定められている一定時間に達した時点で起動する手段を設けたことを特徴とする機密保護方式。

【請求項17】請求項2、4、5、7、8又は9記載の機密保護方式において、スクリーンセーブ手段を設け、タスク制御ブロックまたはタスク制御準備ブロックの利用者識別子フィールドをクリアする制御は、スクリーンセーブが機能した時点で起動する手段を設けたことを特徴とする機密保護方式。

8

【請求項18】請求項2、4、5、7、8又は9記載の機密保護方式において、

該情報処理装置を操作する利用者が、該情報処理装置の操作を中止し、該情報処理装置から離れた離席を検出する離席検出手段を設け、

タスク制御ブロックまたはタスク制御準備ブロックの利用者識別子フィールドをクリアする制御は、離席検出手段により離席が検出された時点で起動する手段を設けたことを特徴とする機密保護方式。

【請求項19】請求項12又は13記載の機密保護方式において、

データにおいて特定の利用者以外のアクセスを禁止するか否かを記述した保護属性には、該利用者を識別する複数の利用者識別子と、該複数の利用者に許可されるアクセスの種類（読み込み、書込み、実行）と、全ての該複数の利用者の利用者識別子が本データのアクセスを行うタスクのタスク制御ブロックに記述されている場合のみ該アクセスを許可する（連動）か否か（非連動）を記述した連動識別子とを設け、

第2の制御手段は、タスクがデータをアクセスする処理を実行する際に、データの保護属性において何れかのアクセスの種類（読み込み、書込み、実行）が不許可とされている場合は、データの保護属性の連動識別子が連動を示していたならば、アクセスするデータの保護属性に記述されている全ての利用者識別子について、一致する利用者識別子がアクセスを行うタスクに対応するタスク制御ブロックに格納されている場合のみ該データのアクセスを許可と判定し、データの保護属性の連動識別子が非連動を示していたならば、アクセスするデータの保護属性に記述されている何れかの利用者識別子と一致する利用者識別子がアクセスを行うタスクに対応するタスク制御ブロックに格納されている場合に該データへのアクセスを許可と判定し、一方、データの保護属性において、全てのアクセスの種類（読み込み、書込み、実行）が許可されている場合は、該データへのアクセスを許可と判定し、その結果、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行することを特徴とする機密保護方式。

【請求項20】請求項6記載の機密保護方式において、タスク制御ブロックは、実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子と、該利用者識別子が有効か無効かを記述した識別子有効フラグを格納し、

第1の制御手段は、第1の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係を、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに、指定された利用者識別子を記述し、ま

9

た、該利用者識別子に対応する識別子有効フラグを有効に設定し、

第2の制御手段は、タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子と、アクセスを行うタスクに対応するタスク制御ブロックにおける識別子有効フラグが有効である利用者識別子とが一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行し、

第4の制御手段、入退室を管理する第2の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、タスク制御ブロックにおいて該利用者識別子と同一の利用者識別子に対応する識別子有効フラグに有効を設定することを特徴とする機密保護方式。

【請求項21】請求項7記載の機密保護方式において、第3の制御手段は、第2の入力手段により機密保護状態の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納し）し、また、識別子有効フラグに無効を設定し、

第2の制御手段は、タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子と、アクセスを行うタスクに対応するタスク制御ブロックにおける識別子有効フラグが有効である利用者識別子とが一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行し、

第5の制御手段は、入退室を管理する第2の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドに対応する識別子有効フラグを無効に設定することを特徴とする機密保護方式。

【請求項22】請求項5又は6記載の機密保護方式において、

第2の情報処理装置に、特定の二つ以上の情報処理装置を示す装置識別子を格納する装置識別子管理テーブルを設け、

第2の情報処理装置の第1の制御手段は、該装置識別子管理テーブルに格納されている装置識別子に対応する情報処理装置へのみ、利用者識別子を第1の情報処理装置に通知することを特徴とする機密保護方式。

10

【請求項23】請求項22記載の機密保護方式において、

装置識別子管理テーブルに格納されている装置識別子に対応する情報処理装置は、特定の部屋内に格納されている情報処理装置であることを特徴とする機密保護方式。

【請求項24】請求項22記載の機密保護方式において、

有線通信を介して他の情報処理装置から受信したデータを無線通信を介して他の情報処理装置へ伝送し、無線通信を介して他の情報処理装置から受信したデータを有線通信を介して他の情報処理装置へ伝送する無線通信装置の装置識別子をデータ装置識別子管理テーブルに格納し、第2の情報処理装置からのデータの送受信を該無線通信装置からの電波の到達範囲に限定することを特徴とする機密保護方式。

【請求項25】請求項24記載の機密保護方式において、

部屋の外部への電波の漏洩を防止した部屋の内部に該無線通信装置を設置し、第2の情報処理装置からのデータの送受信を該部屋内に限定することを特徴とする機密保護方式。

【請求項26】請求項5、6又は7記載の機密保護方式において、

第2の情報処理装置は出退勤管理を行う装置であり、出勤は入室に、退勤は退室に対応することを特徴とする機密保護方式。

【請求項27】請求項5又は6記載の機密保護方式において、

第1の入力手段の入力を行うための専用のキーを設けたことを特徴とする機密保護方式。

【請求項28】請求項5又は7記載の機密保護方式において、

第2の入力手段の入力を行うために専用のキーを設けたことを特徴とする機密保護方式。

【請求項29】請求項19記載の機密保護方式において、

データの保護属性は、連動／非連動の区別を記載した連動識別子を複数記載し、また、該各連動識別子に対応するアクセスの種類（読込み、書込み、実行）と一つ以上の利用者識別子を記載し、

第2の制御手段は、まず、各連動識別子毎に、各連動識別子に対応した利用者識別子とアクセス種類（読込み、書込み、実行）を用いてアクセスの許可／不許可の判定を行い、次に、各連動識別子に対応する結果の論理和でアクセスの許可／不許可を判定することを特徴とする機密保護方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は機密保護機能を有する情報処理装置に係り、特に該不特定多数の利用者が使用する

11

る機会が多い情報処理装置において、特定のデータまたは機能に対する特定の利用者以外のアクセスを制限する場合に好適な機密保護方式及び装置に関する。

【0002】

【従来の技術】情報処理装置において、特定のデータにおける特定の利用者以外のアクセスを制限する機密保護機能を設けることが広く普及している。

【0003】従来の情報処理装置における機密保護機能の第1の従来例としては、特開昭63-249254号において示されているようなものがある。すなわち、利用者情報処理装置を使用するとき、該利用者氏名と暗証番号を入力する。そして、情報処理装置が該利用者氏名と暗証番号の対応関係の一致を確認した後、該利用者は該情報処理装置の使用が可能となる。このように、利用者を唯一に識別する番号または文字列と、該利用者に対応する暗証番号または文字列を入力することにより、情報処理の使用が可能となる方式は、端末装置で広く用いられている。

【0004】前述の従来例は、情報処理装置の利用開始時に利用者氏名、暗証番号等を入力し、特定のデータへのアクセスが可能となる方式であるが、次に示すような第2の従来例もある。つまり、利用者が特定のデータまたは機能へのアクセスを情報処理装置に指示する毎に、該情報処理装置が暗証番号等の入力を該利用者に要求する方式である。

【0005】また、情報処理システムの安全性を高める他の方法として、情報処理装置が設置されている部屋への入退室を管理するものがある。一般には、利用者IDや暗証番号が記録されているカードを、部屋の出入口に設置されているカードリーダーに読み取らせることにより、該出入口の施錠を解除するものである。これにより、該部屋への入室を該カード保有者のみに限定し、他の利用者の情報処理装置の不正利用を防止して、システムの安全性を高めるものである。

【0006】

【発明が解決しようとする課題】上記の第1の従来技術においては、次のような問題点がある。つまり、その情報処理装置を使用しようとする全ての利用者は、利用者氏名、暗証番号等の何らかの入力を行う必要がある、不特定の一般利用者に簡単な操作を提供するのに障害となるという問題点である。特に、該情報処理装置の大部分の利用者は不特定の一般利用者であり、かつ、該情報処理装置には、機密性のあるデータ等特定の利用者のアクセスのみが許されるデータまたは機能が存在する場合には、一般の利用者に適した簡単な操作と、特定の利用者に適した簡単な操作を両立することが難しかった。また、第2の従来技術では、利用者は、特定のアクセスを行う毎に暗証番号等の入力が必要としているので、該情報処理装置を利用する作業の中で、特定のデータまたは機能へのアクセスと、一般のデータまたは機能へのア

12

セスとを頻りに交互に繰り返す場合は、暗証番号等の入力も繰り返す必要があり、操作が煩雑になるという問題点があった。

【0007】また、近年、従来のように情報処理装置を集中して特定の部屋に設置する使用形態は少なくなり、情報処理装置は一般オフィス内に分散して設置されるようになってきた。よって、部屋への入退室を管理しても、情報処理装置を操作しない人々の入室も数多く許可せざるを得なく、それらの人々による情報処理装置の不正使用が為される可能性が否定できないという問題点がある。

【0008】また、複数の業務グループに属する人が情報処理装置の操作をする場合、従来は、同時に複数の業務グループの利用者IDで情報処理装置を操作することが不可能という問題点があった。従来は、グループID等の階層的なIDを導入することによりこの問題点を解決していたが、利用者の所属変更が頻りに行われる場合は、一人の利用者が複数の利用者IDを持つことが実際には多くある。

【0009】本発明は、かかる従来の問題点を解決し、特定の利用者のアクセスのみが許されるデータまたは機能を使用する利用者に適した簡便な操作と、利用者によるアクセスの制限がないデータまたは機能を使用する一般利用者に適した簡便な操作とを両立した機密保護機能の操作方法を実現し、さらに、その機密保護機能を部屋への入退室管理と連携させ、退室した利用者IDによる情報処理装置の不正使用を防止することにある。

【0010】

【課題を解決するための手段】上記目的は、中央処理装置と記憶装置と入力装置と出力装置からなる第1の情報処理装置と、入退室管理を行うための第2の情報処理装置からなるシステムにおいて、次に述べる手段を設けることにより達成される。

【0011】まず、第1の情報処理装置に以下の手段を設ける。

【0012】(1)データの所有者を識別する利用者識別子と、所有者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータ。

【0013】(2)実行中の各タスクに対応して設け、該タスクの利用者を唯一に識別する利用者IDを格納したタスク制御ブロック。

【0014】(3)利用者IDと暗証番号の対応関係を記述した暗証番号管理テーブル。

【0015】(4)利用者が、他人へのアクセスを禁止したデータをアクセスするために、利用者IDと暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除（アンロック）を該情報処理装置に指示する第1の入力手段。

【0016】(5)利用者が、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすると

13

を禁止する状態にするために、第1の入力手段を用いた指示により解除された機密保護状態を解除前の状態に戻す、つまり、機密保護状態を設定する(ロック)指示を行う第2の入力手段。

【0017】(6) 第1の入力手段による入力が行われたときに、利用者IDと暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者IDフィールドに、指定された利用者IDを記述する第1の制御手段。

【0018】(7) タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者IDとアクセスを行うタスクに対応するタスク制御ブロックの利用者IDが一致するか否かを検査し、また、データの保護属性を参照して、利用者IDが不一致かつ保護属性が所有者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第2の制御手段。

【0019】(8) 第2の入力手段により機密保護状態の設定(ロック)の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者IDフィールドをクリア(一般の利用者を示す利用者IDを格納する)する第3の制御手段。

【0020】(9) 入退室を管理する第2の情報処理装置から、退室した利用者の利用者IDが通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者IDと同一の利用者が格納されている利用者IDフィールドをクリア(一般の利用者を示す利用者IDを格納する)する第4の制御手段。

【0021】(10) 入退室を管理する第2の情報処理装置から、入室した利用者の利用者IDが通知されたならば、実行中のタスクに対応するタスク制御ブロックの利用者IDフィールドに該利用者IDを格納する第5の制御手段。

【0022】次に、第2の情報処理装置に以下の手段を設ける。

【0023】(11) 入室する利用者の利用者IDを入力する第1の入力手段。

【0024】(12) 退室する利用者の利用者IDを入力する第2の入力手段。

【0025】(13) 入室する利用者の利用者IDが第1の入力手段により入力されたならば、該利用者IDの利用者IDを入室した利用者の利用者IDとして、第1の情報処理装置に通知する第1の制御手段。

【0026】(14) 退室する利用者の利用者IDが第2の入力手段により入力されたならば、該利用者IDの利用者IDを退室した利用者の利用者IDとして、第1

14

の情報処理装置に通知する第2の制御手段。

【0027】

【作用】第1の情報処理装置において、利用者が、第1の入力手段により、他人へのアクセスを禁止したデータをアクセスするために、利用者IDと暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除(アンロック)を該情報処理装置に指示したならば、第1の制御手段により、利用者IDと暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者IDフィールドに、指定された利用者IDを記述する。

【0028】また、第1の情報処理装置において、利用者が、第2の入力手段により、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすることを禁止する状態にするために、第1の入力手段を用いた指示により解除された機密保護状態を解除前の状態に戻す、つまり、機密保護状態を設定する(ロック)指示を行ったならば、第3の制御手段により、実行中のタスクに対応するタスク制御ブロックの利用者IDフィールドをクリア(一般の利用者を示す利用者IDを格納する)する。

【0029】また、第1の情報処理装置において、タスクがデータをアクセスする処理を実行する際には、第2の制御手段により、アクセスするデータの利用者IDとアクセスを行うタスクに対応するタスク制御ブロックの利用者IDが一致するか否かを検査し、また、データの保護属性を参照して、利用者IDが不一致かつ保護属性が所有者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する。

【0030】また、第1の情報処理装置において、入退室を管理する第2の情報処理装置から、退室した利用者の利用者IDが通知されたならば、第4の制御手段により、実行中のタスクに対応するタスク制御ブロックで該利用者IDと同一の利用者が格納されている利用者IDフィールドをクリア(一般の利用者を示す利用者IDを格納する)する。

【0031】また、第1の情報処理装置において、入退室を管理する第2の情報処理装置から、入室した利用者の利用者IDが通知されたならば、第5の制御手段により、実行中のタスクに対応するタスク制御ブロックの利用者IDフィールドに該利用者IDを格納する。

【0032】また、第2の情報処理装置において、入室する利用者の利用者IDが第1の入力手段により入力されたならば、第1の制御手段により、該利用者IDの利用者IDを入室した利用者の利用者IDとして、第1の

15

情報処理装置に通知する。

【0033】また、第2の情報処理装置において、退室する利用者の利用者IDが第2の入力手段より入力されたならば、第2の制御手段により、該利用者IDの利用者IDを退室した利用者の利用者IDとして、第1の情報処理装置に通知する。

【0034】このように、特定の利用者のアクセスのみが許されるデータまたは機能を使用する利用者に適した簡便な操作と、利用者によるアクセスの制限がないデータまたは機能を使用する一般利用者に適した簡便な操作とを両立した機密保護機能の操作方法を実現し、さらに、その機密保護機能を部屋への入室管理と連携させ、退室した利用者IDによる情報処理装置の不正使用を防止することができる。

【0035】

【実施例】以下、本発明の一実施例を図面を用いて説明する。

【0036】まず、図1と図2を用いて本システム構成と使用環境を説明する。100は情報処理装置を設置または使用する部屋であり、電波を遮断する素材を用いた構造となっている。該部屋100の入口101には、部屋の内側と外側に入室管理装置111がある。該部屋内には、情報処理装置110と無線LAN制御装置112が設けられている。各情報処理装置110、入室管理装置111、無線LAN制御装置112は、互いにLAN113または無線通信により接続されており、各装置110～112間でデータ通信が可能である。なお、無線通信は、無線LAN制御装置112と無線通信用のアンテナをもつ該部屋内にある情報処理装置110の間で行われる。無線LAN制御装置112は、部屋の外にある情報処理装置110との間では通信を行うことができない。各装置110～112は、ディスプレイ装置や通信装置の有無という多少の差があるが、ほぼ同一のハードウェア構成を有する。なお、入室管理装置111は、部屋の内部に設けられるカードリーダー11aと、部屋の外部に設けられるカードリーダー11bが接続される。カードリーダー11a、bは、カード114へのデータの書き込みまたは読み出しが可能である。

【0037】次に、図3を用いて、各装置110～112のハードウェア構成について説明する。301は中央処理ユニット(CPU)であり、各種の処理プログラムの実行、及び周辺機器302～309の制御を行う。302は主メモリ(M)であり、機密保護機能を初めとする各種の処理プログラム及びデータが格納される。機密保護機能を初めとする各種の処理プログラムに対する指示は、キーボード306(KB)、マウス307を介して行われる。305はディスプレイ装置(D)であり、機密保護機能を初めとする各種の処理プログラムに関する画面をマルチウィンドウの形式で表示する。30

16

4はフロッピーディスク装置(FDD)であり、各種のデータの読み出しや保存を行う。303は固定ディスク装置(HDD)であり、各種のデータの読み出しまたは保存を行う。310はこれらの周辺機器302～309と中央処理ユニット301間のデータ転送を行なうためのバスである。

【0038】次に、図4を用いて、本実施例のソフトウェア構成について説明する。401a～eは、本実施例の情報処理装置に各種の処理タスクである。401a～eは各々独立したタスクとしてマルチタスクオペレーティングシステムプログラム(以下OSと略す)400で制御される。また、タスク401eは機密保護機能に係るタスクである。OS400は、基本的なタスク制御や入出力制御から、ディスプレイ装置305の画面上でマルチウィンドウを実現する制御、後で述べるファイルをアクセスする制御、機密保護機能に係る制御等を行う。

【0039】次に、図5を用いて、本実施例の情報処理装置における機密保護機能の処理機構について説明する。機密保護機能は、情報処理装置110上で動作する各種のタスク401が、固定ディスク装置303に格納されているファイル600にアクセスする場合に、タスク401のファイルアクセス要求処理501によって呼び出されたOS400のファイルアクセス処理502が、ファイル600の利用者ID630とタスク制御ブロック800の利用者ID810の照合を行い、ファイル600のファイル保護属性30に従って、タスク401によるファイル600のアクセスを制限するものである。そして、タスク制御ブロック800の利用者ID810は、キー入力507等の利用者の指示によって呼び出された各種の機密保護タスク401eのアンロック要求503や、アンロックを指示するデータの受信506等により、OS400のアンロック処理504が呼出され、該アンロック処理504がタスク制御ブロック800の利用者ID810を設定する。なお、キー507は、キーボード306に設けられているものであり、アンロック等の機密保護機能を起動するための専用キーである。キー507には、アンロックを指定する専用キー507aとロックを指定する専用キー507bがそれぞれ設けられている。専用キーを設けることにより、利用者はアンロック、ロックの機能を容易に見分けることができ、よって、利用機会が増加かつ普及するとともに、同時に該機能を起動することができる。

【0040】次に、図6と図7を用いて、本実施例に係るファイルのデータ構造について説明する。ファイル600は、ファイル名称610、ファイル保護属性620、利用者ID630、及びデータ640からなり、各種のデータや実行可能な処理プログラムが格納される。ファイル名称610は、該ファイル600の名称を示す。ファイル保護属性620は、該ファイル600の読み書き実行を利用者により制限するためのもので、該フ

17

ファイル600の所有者以外の利用者に対する読込みの可／不可621、書き込みの可／不可622、実行の可／不可623が記憶されている。利用者ID630は、該ファイル600の所有者を唯一に識別する。データ640は、文書等の各種のデータや実行可能な処理プログラムのデータ本体である。

【0041】次に、タスク制御ブロックについて図8を用いて説明する。タスク制御ブロック800は、OS400により制御されている各タスク400に対して一個づつ設けられ、該タスクを利用している利用者を識別する利用者ID810と該利用者ID810が有効か無効かを示すID有効フラグ820を格納する。OS400は、タスク400の起動に際して、タスク制御ブロック800を生成する。また、OS400は、タスク401が終了、消滅すると同時に、対応するタスク制御ブロック800を削除する。

【0042】次に、増設番号管理テーブルについて、図9を用いて説明する。増設番号管理テーブル900は、各利用者ID910と、該各利用者ID910に対して設定された増設番号930との対応関係が格納される。

【0043】次に、ウィンドウ管理データについて図10と図17を用いて説明する。ウィンドウ管理データ1000には、ディスプレイ装置305の画面1700上に表示されている各ウィンドウ1710について、該ウィンドウ1710を表示しているタスク401のタスク制御ブロック800が記憶されている主メモリ302上のアドレス1010が記憶されている。また、ディスプレイ装置305の画面1700上でアクティブな状態で表示されているアクティブウィンドウ（図17の例では1710c）を示すために、アクティブウィンドウポインタ1020が、該アクティブウィンドウ1710cに対応するタスク制御ブロック800のアドレス1010が記憶されているウィンドウ管理データ1000中の位置を示している。

【0044】次に、入退室管理装置111の入退室処理について図11、図12、図14を用いて説明する。入退室処理1100は、利用者が入退室管理装置111のカードリーダー111a、bに、カード111より、利用者IDを入力すると（1101）、入退室管理テーブル1200を更新し（1102）、入退室があったことを示すデータを、装置管理テーブル1150に記憶されている各装置ID1155に対応する情報処理装置110に送信する（1103）。装置管理テーブル1150は、各情報処理装置110を唯一に識別するIDを複数格納することができ、一般には、該部屋100内に設置されている各情報処理装置110と無線通信装置112の装置ID1155を格納する。これにより、以下で述べる利用者の入退室に係る機密保護機能は、該部屋100内に設置されている情報処理装置110～112の不正使用防止に限られる。但し、入退室管理装置11

18

1を出退勤管理に使用する例も考えられ、その場合は部屋100とは関係無く、従業員の使用する各情報処理装置の装置IDを装置管理テーブル1150に記憶することにより、他人が既に退勤している従業員の利用者IDを用いて該情報処理装置110を不正使用することが防止できる。また、部屋100内のカードリーダー111aにより、入力が行われた場合は退室と判断し、部屋100外のカードリーダー111bにより、入力が行われた場合は入室と判断する。入退室管理テーブル1200は、各利用者ID1201に対する入退室状況（入室中／退室後）1202が記憶される。つまり、入室があった利用者ID1201の入退室状況1202には入室と記憶され、退室があった利用者ID1201の入退室状況1202には退室と記憶される。なお、入退室処理1100は、制御処理1400により、カードによる入力があった場合に起動される（1410、1430）。

【0045】次に、入退室管理装置111の入退室状況問い合わせ処理について、図12、図13、図14を用いて説明する。入退室状況問い合わせ処理1300は、制御処理1400により、他の情報処理装置110から、ある利用者が入室中か否かを問い合わせるデータを受信した場合に起動される（1410、1420）。入退室状況問い合わせ処理1300は、まず、問い合わせの対象となる利用者IDを受信し（1320）、該利用者ID1201に対応する入退室状況1202を入退室管理テーブル1200から取得する（1320）。そして、該入退室状況1202を問い合わせ元の情報処理装置110に返信する（1330）。

【0046】次に、機密保護設定画面について図15を用いて説明する。機密保護設定画面1500は、利用者が、ファイル600に対して、他人の読込み、書込み、実行を禁止する保護属性を設定するための画面である。そして、機密保護設定画面1500は、図17に示すように、一つのウィンドウ1710としてディスプレイ装置305の画面1700上に表示される。また、この画面1500は、例えば文書の編集終了時等、文書データをファイル600として格納するときや、利用者が該ファイル600に機密保護の設定を要求した場合に表示される。また、利用者が既存のファイル600に対して、機密保護の設定または解除を要求した場合にも表示される。そして、該ファイル600において他人の読込みを禁止する場合は、選択項目1515をマウス307を用いて指示する。一方、他人の読込みを許可する場合は、選択項目1510を指示する。また、他人の書込みを禁止する場合は、選択項目1525をマウス307を用いて指示する。一方、他人の書込みを許可する場合は、選択項目1520を指示する。また、他人の実行を禁止する場合は、選択項目1535をマウス307を用いて指示する。一方、他人の実行を許可する場合は、選択項目1530を指示する。さらに、後に述べるロック状態で

19

は、利用者ID1540と暗証番号1550の入力欄が表示され、利用者による利用者IDと暗証番号の入力を必要とする。

【0047】次に、アンロック画面について図16を用いて説明する。アンロック画面1600は、利用者が自分以外の人の読みまたは書き込みを禁止されているファイルを利用する時に、情報処理装置110に該利用者の利用者IDを通知することによって、該利用者の読み込み、書き込み、または、実行を可能にするため指示を行う画面である。そして、アンロック画面は、図17に示すように、一つのウィンドウ1710としてディスプレイ装置305の画面1700上に表示される。1610は利用者IDの入力欄、1620は暗証番号の入力欄であり、利用者による利用者IDと暗証番号の入力を必要とする。

【0048】次に、本文処理装置のディスプレイ装置305の画面上における表示の一例を図17を用いて説明する。1710は各タスク401が表示するウィンドウである。なお、ある時点においては、画面1700上で一つだけのウィンドウ1710がアクティブな状態となる。アクティブな状態とは、キーボード306またはマウス307による入力が、該ウィンドウ1710に対して、つまり、該ウィンドウ1710を表示しているタスク401に対して行われることを意味している。1720は、後に述べるアンロック操作によって表示されるアンロック表示であり、現在、ある利用者に対する読み込み、書き込み、または実行の禁止が解除されていることを示す。1721は、1720と同様のアンロック表示であり、表示中のウィンドウ1710の中に1つ以上のアンロック表示1720が行われているウィンドウ1710がある場合に表示される。各ウィンドウ1710内のあるタスク401がウィンドウの重なりにより見えなくなり、アンロック状態であることが分からなくなること防止するために1721も表示する。上述の画面表示例では、アンロックの状態を示すために1720を表示したが、ウィンドウ枠の色をアンロックの状態を示す特定の色に変える実施例も考えられる。

【0049】次に、以上で述べたシステム構成からなる情報処理装置における、機密保護関係の処理について説明する。

【0050】まず、ファイルアクセスを制限する機構について、図18を用いて説明する。タスク401は、ファイルアクセスをOS400に要求すると、該OS400のファイルアクセス処理502は、まず、ファイル600のアクセスが許されるか否かの検査を行い(1810)、次に、ファイルアクセス(1820)を行う。アクセス許可検査処理1810は以下の処理を行う。まず、アクセスするファイル600のファイル保護属性620と利用者ID630を取得し、該ファイル保護属性620の各属性621〜623の何れかに不可の指定が

20

ある場合は、以下の処理を行う。すなわち、ファイルアクセスを要求したタスク401に対応するタスク制御ブロック800の1D有効フラグ820を参照し、該1D有効フラグ820が有効を示していたならば、該タスク制御ブロック800の利用者ID810を取得する。そして、該利用者ID810とファイル600の利用者ID630が一致しない場合は、ファイル保護属性620で不可が示されている種類のアクセスが禁止される。ファイル保護属性620で可が示されている種類のアクセスが可能である。なお、1D有効フラグ820が無効を示していたならば、ファイル保護属性620に関係なく、全ての種類のアクセスが可能である。

【0051】次に、利用者指示によって起動されるアンロック機能について、図19を用いて説明する。本実施例におけるアンロックとは、利用者が自分以外の人の読み込み、書き込み、または、実行を禁止した文書ファイルを利用する時に、情報処理装置110に該利用者の利用者IDを入力することによって、該利用者の読み込み、書き込み、または、実行を可能にすることである。アンロック機能は、機密保護タスク401eのアンロック処理1900とOSのアンロック処理504aにより実現される。

【0052】まず、機密保護タスク401eのアンロック処理1900について説明する。アンロック処理1900は、利用者がキーボード306上のアンロックキー507aを押した場合に、OS400によって起動される。アンロック処理1900は、図16に示すアンロック画面1600をディスプレイ装置305の画面に表示し、利用者から利用者IDと暗証番号の入力を受け付ける(1910)。次に、入室中以外の利用者によるアンロックを禁止するために、入退室管理装置111へ処理1910で取得した該利用者IDの利用者が入室中であるか否かを問い合わせ、入室中以外の場合は処理を終了する(1920)。次に、暗証番号管理テーブル900を参照し、1910の処理で入力された利用者IDと暗証番号の対応関係が、該暗証番号管理テーブル900に記述されている利用者ID910と暗証番号930の対応関係と一致しているか否かを検査する(1930)。不一致の場合は処理を終了し、一致している場合は、OS400のアンロック処理を起動する(1940)。

【0053】次に、OS400のアンロック処理504aについて説明する。OS400のアンロック処理504aは、ディスプレイ装置305の画面1700上にアクティブな状態で表示されているウィンドウ1710を表示しているタスク401に関してアンロックの処理を行う。機密保護タスク401eのアンロック処理1900における1940の処理によって起動されたアンロック処理504aは、まず、ウィンドウ管理データ100を参照し、アクティブな状態で表示されているウィンドウ1710を表示しているタスク401のタスク制御

21

ブロック800のアドレス1010を取得する(1950)。次に、機密保護タスク401eの処理1910で入力した利用者IDを該タスク制御ブロック800の利用者ID810として設定し、また、ID有効フラグ820を有効に設定する(1960)。また、該アクティブな状態のウインドウ1710にアンロック表示1720、1721の表示1722を行う(1970)。
【0054】上述の実施例では、アンロックキー507aを押したとき、アンロックはアクティブな状態のウインドウ1710を表示しているタスク401に対して行われたが、アクティブな状態でないウインドウ1710に関してアンロックを行う場合は、アンロックを行うおとすウインドウ1710をアクティブな状態にして(アクティブ)からアンロックキー507aを押す必要がある。

【0055】次に、利用者指示によって起動されるロック機能について、図20を用いて説明する。本実施例におけるロックとは、先に述べたアンロックの逆の操作であり、読み込み、書き込み、または実行を禁止したファイル600に対するアクセスを不可能にすることである。ロック処理505aは、利用者がキーボード306上のロックキー507bを押した場合に起動されるOS400の処理である。ロック処理505aは、まず、ウインドウ管理データ1000を参照し、アクティブな状態で表示されているウインドウ1710を表示しているタスク401のタスク制御ブロック800のアドレス1010を取得する(2110)。次に、該タスク制御ブロック800に設定されている利用者ID810をクリア(一般利用者を示す利用者IDをセットする)する。(1220)。また、該アクティブな状態のウインドウ1710に表示されているアンロック表示1720を消去する(2130)。その際に、アンロック表示1720を行っている(アンロックの状態である)他のウインドウ1710がなければ、1721のアンロック表示も消去する。また、ウインドウ1710をクローズすることにより、該ウインドウ1710を表示しているタスク401を終了すると、OS400が該タスク401に対応するタスク制御ブロック800を削除する。

【0056】上述の実施例では、ロックキー507bを押したとき、ロックは、アクティブな状態のウインドウ1710を表示しているタスク401に対して行われたが、アクティブな状態でないウインドウ1710に関してロックを行う場合は、ロックを行うおとすウインドウ1710をアクティブな状態にして(アクティブ)からロックキー507bを押す必要がある。

【0057】次に、入退室管理装置111が利用者の退室を検出し、そのことを各情報処理装置110に通知した場合の各情報処理装置110のロック処理について、図21を用いて説明する。情報処理装置110が入退室管理装置111から退室データを受信すると、OS400

22

0は、ロック処理505bを起動する。ロック処理505bは、まず、退室した利用者の利用者IDを取得し(2110)、該利用者IDと同一の利用者ID810を有する全てのタスク制御ブロック800のID有効フラグ820を無効に設定する(2120)。そして、ディスプレイ装置305の画面1700上に表示されているアンロック表示1720を消去する(2130)。

【0058】次に、入退室管理装置111が利用者の入室を検出し、そのことを各情報処理装置110に通知した場合の各情報処理装置110のアンロック処理について、図22を用いて説明する。情報処理装置110が入退室管理装置111から入室データを受信すると、OS400は、アンロック処理504bを起動する。アンロック処理504bは、まず、入室した利用者の利用者IDを取得し(2210)、該利用者IDと同一の利用者ID810を有する全てのタスク制御ブロック800のID有効フラグ820を有効に設定する(2220)。そして、ディスプレイ装置305の画面1700上にアンロック表示1720を表示する(2230)。

【0059】次に、機密保護設定処理について図23を用いて説明する。機密保護設定処理2300は、ファイル600に対して他人の読書き実行を制限することを利用者が要求した場合に呼び出される。機密保護設定処理2300は、まず、ウインドウ管理データ1000を参照し、アクティブな状態で表示されているウインドウ1710を表示しているタスク401のタスク制御ブロック800のアドレス1010を取得する(2310)。次に、該タスク制御ブロック800に設定されている利用者ID810を参照する(2320)。そして、図15に示した機密保護設定画面1500を表示し、利用者が入力したファイル保護属性1510～1535、利用者ID1540、暗証番号1550を取得し(2330)、ファイル保護属性と利用者IDをファイル600の利用者ID630に設定する。但し、2330の処理は、該タスク制御ブロック800に設定されている利用者ID810が、一般利用者を示す利用者IDである場合のみ、利用者IDの入力欄1540と暗証番号の入力欄1550を表示し、利用者に入力要求する。それ以外の場合は、2340の処理でファイル600に設定される利用者ID630は、2320の処理で取得したタスク制御ブロック800の利用者ID810である。

【0060】上述の各実施例では、アンロックキー507aの押下時に、アクティブな状態にあるウインドウ1710を表示しているタスク401に関してのみアンロックを行ったが、該情報処理装置110で動作する特定の一部分または全てのタスク401に関してアンロックを行う実施例も考えられる。この場合、利用者は、アンロックを行った後、該情報処理装置で動作する全てのタスク401の利用者に関して、該利用者以外に対してアクセス制限のあるファイル600がアクセス可能となる。

23

また、この場合は、ロックは、該情報処理装置110で動作する特定の一部分または全てのタスク401に関してロックを行う。

【0061】以上で述べた実施例によれば、情報処理装置110における利用者に対する機密保護状態の解除（アンロック）、及び、機密保護状態の設定（ロック）を、タスク401の実行中など利用者が希望する任意の時点で行うことを可能にし、機密保護状態が設定（ロック）されている状態では、アクセスが禁止されているファイル600へのタスク401のアクセスを禁止することで、特定の利用者のアクセスのみが許されるファイル600を使用する利用者に適した簡便な操作と、利用者によるアクセスの制限がないファイル600を使用する一般利用者に適した簡便な操作とを両立した機密保護機能の操作方法を実現することができる。また、該ロック、アンロック機能を情報処理装置110が設置されている部屋100の入退室管理機能と組み合わせることで、他人が退室した人の利用者IDを用いて情報処理装置110を不正に使用することを防止することができる。

【0062】また、以上の実施例を改良した次のような実施例も考えることができる。

【0063】まず、各タスク制御ブロック800に、複数組の利用者ID811とID有効フラグ821を格納できるようにする。また、図1に示したアクセス許可検査処理1810においては、タスク制御ブロック800を参照し、ID有効フラグ821が有効を示している全ての利用者ID811の中にファイル600の利用者ID630と一致するものがない場合に、ファイル保護属性620で可が示されている種類のアクセスを禁止する。但し、ファイル保護属性620で可が示されている種類のアクセスは可能である。なお、全てのID有効フラグ821が無効を示していたならば、ファイル保護属性620に関係無く、全ての種類のアクセスが可能である。また、図19におけるタスク制御ブロック19設定の処理1960では、利用者ID811とID有効フラグ821を追記するようになる（既に記述されている利用者ID811とID有効フラグ821に重ね書きしない）。

【0064】また、以上の実施例を改良した次のような第2の実施例がある。第一の実施例では、利用者の指示と、入退室をきっかけとしてアンロック/ロックを行ったが、次に示すようなイベントを、アンロック/ロックのきっかけとして、単独または併用して用いてもよい。

【0065】図26を用いて説明する。ロック処理505を起動する処理として、離席検出処理2610、初期画面表示処理2620、無入力検出処理2630、スクリーンセーブ表示処理2640がある。

【0066】離席検出処理2610は、図27に示す、情報処理装置110に設置された離席検出装置2700

24

が検出した利用者の離席状態が、予め定められた一定時間に達し、かつ、アンロック状態のタスクが存在する場合（ID有効フラグ820に有効が設定されているタスク制御ブロック800がある場合）に、ロック処理505を起動する。これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。離席検出装置2700は、ディスプレイ装置305の前方にある物体との距離を防止する超音波測距装置であり、測定距離が予め定められている一定距離を超えた場合に、該情報処理装置110の利用者が離席したと判断する。初期画面表示処理2620は、その情報処理装置で実行可能な機能の一覧を表示し、実行する機能を選択する初期画面を表示している状態が、予め定められた一定時間に達し、かつ、アンロック状態のタスク401が存在する場合（ID有効フラグ820に有効が設定されているタスク制御ブロック800がある場合）に、ロック処理505を起動する。初期画面とは、情報処理装置110の電源投入後最初に表示される画面1700であって、該情報処理装置110で使用可能な機能の選択画面が表示される。利用者が情報処理装置110の操作を終了または中断する場合、該画面を表示した状態にして、該情報処理装置110を放置する場合が多い。よって、これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。無入力検出処理2630は、キーボード306、マウス307の無入力状態が、予め定められた一定時間に達し、かつ、アンロック状態のタスクが存在する場合（ID有効フラグ820に有効が設定されているタスク制御ブロック800がある場合）に、ロック処理505を起動する。これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。スクリーンセーブ表示処理2640は、焼き付き防止画面の表示開始と同時に、アンロック状態のタスクが存在する場合（ID有効フラグ820に有効が設定されているタスク制御ブロック800がある場合）に、ロック処理505を起動する。これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。なお、本第2の実施例は、以下で述べる実施例でも適用できる。

【0067】また、以上の実施例を改良した次のような第3の実施例がある。第一の実施例では、利用者の指示や入退室等のイベントがあった時点でロック処理を行ったが、次に示すように、ある単位の処理が終了するまでロック処理の起動を保留してもよい。

【0068】まず、予備制御テーブルについて、図29を用いて説明する。予備制御テーブル2900は各タスク制御ブロック800に対応して設け、タスク制御ブロック800と同様に、利用者ID2910とID有効フ

25

ラグ2920を設ける。
【0069】つぎに、ロック一時保留機構について、図28を用いて説明する。

【0070】第一の実施例で述べた各ロック処理505において、タスク制御ブロック800の利用者ID810を削除したり、ID有効フラグ820を無効に設定する処理では、第1の実施例でタスク制御ブロック800に対して行ったのに代わって、予備制御テーブル2900に対して行う。そして、アクセス制御データ整合処理2800が、指定されたタスク401に対応する予備制御テーブル2900に記述されている利用者ID2910とID有効フラグ2920の状態を、タスク制御ブロック800に設定する。つまり、ロックが指示された時点では、タスク制御ブロック800を操作してロック状態にしないで、アクセス制御データ整合処理2800が動作した時点で、タスク制御ブロック800を操作してロック状態にする。アクセス制御データ整合処理2800は、図30に示すように、3つの処理3010、3020から起動する場合が考えられる。各処理3010、3020からの起動を単独に用いても、併用しても良い。また、各処理3010、3020は、アクセス制御データ整合処理2800を起動する際に、アクセス制御データ整合処理2800の処理対象となるタスク401を唯一に識別するタスクIDを、パラメータとしてアクセス制御データ整合処理2800に通知する。

【0071】ファイルクローズ処理3010は、OS400の処理であり、オープンしたファイル600をクローズする処理を行う際に、アクセス制御データ整合処理2800を起動し、ファイルのクローズを要求したタスクのタスクIDを、該アクセス制御データ整合処理2800に通知する。

【0072】タスク終了処理3020は、OS400の処理であり、タスク401を終了する処理を行う際に、アクセス制御データ整合処理2800を起動し、終了するタスクのタスクIDを、該アクセス制御データ整合処理2800に通知する。

【0073】第3の実施例では、ファイルのアクセスやタスクの処理が終了するまでロックの処理を一時保留することで、ファイルのアクセス中やタスクの実行中に利用者が退室したり、離席した場合にも、該ファイルのアクセスやタスクの実行が中断して異常終了となることを防止している。なお、本第3の実施例は、以下で述べる実施例でも適用できる。

【0074】また、以上の実施例を改良した次のような第4の実施例がある。複数の利用者に対して同時に機密保護状態の解除（アンロック）を行うことが可能な実施例である。

【0075】まず、各タスク制御ブロック800に、複数の利用者ID811とID有効フラグ821を格納できるようにする。また、図18に示したアクセス許可

26

検査処理1810においては、タスク制御ブロック800を参照し、ID有効フラグ821が有効を示している全ての利用者ID811の中にファイル600の利用者ID630と一致するものが無い場合は、ファイル保護属性620で不可が示されている種類のアクセスを禁止するようにする。但し、ファイル保護属性620で可が示されている種類のアクセスは可能である。なお、全てのID有効フラグ821が無効を示していたら、ファイル保護属性620に関係無く、全ての種類のアクセスが可能である。また、図19におけるタスク制御ブロックID設定の処理1960では、利用者ID811とID有効フラグ821を追記するようにする（既に記述されている利用者ID811とID有効フラグ821に重ね書きしない）。また、図20で示したロック処理の代わりに、新たに図32に示すロック処理を設ける。利用者によりロックキーが入力されたならば、機密保護タスク401eのロック処理3200がOS400によって起動される。ロック処理3200は、図33に示すロック画面3100を表示して、利用者によって利用者ID入力欄3110に入力される利用者IDを取得した後、OS400のロック処理505aを起動する。ロック処理505aは、まず、ウィンドウ管理データ1000を参照し、アクティブな状態で表示されているウィンドウ1710を表示しているタスク401のタスク制御ブロック800のアドレス1010を取得する（1950）。次に、該タスク制御ブロック800に設定されている利用者ID810の中で、処理3210で取得した利用者IDと同一の利用者ID811が記述されている利用者ID811とその有効フラグ821のフィールドを削除する（1960）。また、1960の処理を行った結果、各タスク制御ブロックについて、該タスク制御ブロック800に記述されている利用者ID811が無くなった場合は、該タスクが表示しているウィンドウ1710におけるアンロック表示1720を消去する（1970）。さらにその結果、アンロック表示1720を行っている（アンロックの状態である）ウィンドウ1710が無くなれば、1721のアンロック表示も消去する。また、ウィンドウ1710をクローズすることにより、該ウィンドウ1710を表示しているタスク401を終了すると、OS400が該タスク401に対応するタスク制御ブロック800を削除するので、ロックと同じ効果がある。

【0076】また、図22で示した入室データ受信によるアンロック処理と、図21で示した退室データ受信によるロック処理にも、同様な多重方式への変更を行う。つまり、図22におけるタスク制御ブロック有効フラグセットの処理2220では、全てのタスク制御ブロック800に関して、2210の処理で取得した利用者IDと一致する全ての利用者ID811に対応するID有効フラグ821を有効に設定する。また、図21における

タスク制御ブロック無効フラグセットの処理2120では、全てのタスク制御ブロック8000に関して、処理2110で取得した利用者IDと一致する全ての利用者ID811に対応する有効フラグ821のフィールドを無効にセットする。また、2120の処理を行った結果、各タスク制御ブロックについて、該タスク制御ブロック8000に記述されている利用者ID811の中で有効フラグ821が有効に設定されているものが無くなった場合は、該タスクが表示されているウィンドウ1710におけるアンロック表示1720を消去する(2130)。さらにその結果、アンロック表示1720を行っている(アンロックの状態である)ウィンドウ1710が無くなれば、1721のアンロック表示も消去する。

【0077】この第2の実施例では、第1の実施例での効果に加えて、同一の情報処理装置110または同一のタスク401において、複数の利用者に対して同時に機密保護状態の解除(アンロック)を行うことができる。つまり、ファイルAのアクセスが利用者Aに許可されていて、ファイルBのアクセスが利用者Bに許可されている場合、利用者A、Bについてアンロックを行えば、ファイルAとファイルBのアクセスが同時に行える。これは、一人の利用者が、例えばA委員会メンバーとしての利用者IDとB委員会メンバーとしての利用者ID等、2つ以上の利用者IDを持つ場合の操作に便利方式である。グループIDを設ける方式もあるが、グループの再編分割、所属変更が頻繁に行われる場合は、本実施例のように、一人の利用者が2つ以上の利用者IDを持てる方式の方が現実的に対処できる。

【0078】また、以上の実施例を改良した次のような第5の実施例がある。同一のファイルアクセスに対して、二人以上の利用者に対する機密保護状態の解除(アンロック)を必要とするようにできる方式である。

【0079】まず、図6に示したファイル600のファイル保護属性620を、図25に示す構造に変更し、図6の利用者ID630を廃止する。つまり、複数の保護属性625を記述できるようにし、各保護属性625には、連動属性624と一つ以上の利用者ID626を記述できるようにする。連動属性624には、連動/非連動の区別が記述される。連動と記述されている場合は、同一のファイル保護属性625に記述されている各機密保護属性621〜623で不可と設定されているアクセスが可能になる状態は、情報処理装置110が同一のファイル保護属性625に記述されている全ての利用者ID626に対してアンロック状態になっている場合に限られる。一方、非連動と記述されている場合は、同一のファイル保護属性625に記述されている各機密保護属性621〜623で不可と設定されているアクセスが可能になる状態は、情報処理装置110が同一のファイル保護属性625に記述されているいずれかの利用者ID626に対してアンロック状態になっている場合であ

る。そして、第1の実施例において、図18で示したファイルアクセス制限機構のアクセス許可検査1810を、上述のファイル保護属性620に適合するように変更する。

【0080】この第5の実施例では、あるファイルのアクセス(特に、処理プログラムが格納されているファイルの実行)に際して、複数の利用者に対してアンロック状態とすることを必要とすることができる。つまり、例えば、工業プラントの始動等、そのファイル(処理プログラム)の実行が重大な結果を生む可能性のある場合、一人の軽率な判断でなく複数の利用者の判断の下での実行を要し、システムの安全性を高めることができる。

【0081】

【発明の効果】以上述べたように、本発明によれば、情報処理装置の利用者に対する機密保護状態の解除(アンロック)、及び、機密保護状態の設定(ロック)を、利用者が希望する任意の時点で行うことが可能にし、また、該情報処理装置が設置されている部屋への利用者の入退室や、該情報処理装置の操作の中断とリンクして、ロックとアンロックを行う。そして、ロックされている状態では、アクセスが禁止されているファイルのアクセスを禁止することで、ファイルの不正利用を防止することができる。

【図面の簡単な説明】

【図1】システムの使用環境説明図である。

【図2】システム構成図である。

【図3】情報処理装置のハードウェア構成図である。

【図4】情報処理装置のソフトウェア構成図である。

【図5】情報処理装置の機密保護機構の説明図である。

【図6】ファイルのデータ構造の説明図である。

【図7】ファイル保護属性のデータ構造の説明図である。

【図8】タスク制御ブロックのデータ構造の説明図である。

【図9】暗証番号管理テーブルのデータ構造の説明図である。

【図10】ウィンドウ管理データのデータ構造の説明図である。

【図11】入退室管理装置の入退室処理の説明図である。

【図12】入退室管理装置における入退室管理テーブルのデータ構造の説明図である。

【図13】入退室管理装置の入退室状況問い合わせ処理の説明図である。

【図14】入退室管理装置の制御処理の説明図である。

【図15】機密保護設定画面の表示例を示す図である。

【図16】アンロック画面の表示例を示す図である。

【図17】ディスプレイ装置の画面表示例を示す図である。

【図18】ファイルアクセス制限機構の説明図である。

29

【図19】利用者指示によるアンロック処理の説明図である。

【図20】利用者指示によるロック処理の説明図である。

【図21】退室データ受信によるロック処理の説明図である。

【図22】入室データ受信によるアンロック処理の説明図である。

【図23】機密保護設定処理の説明図である。

【図24】第4の実施例に係るタスク制御ブロックのデータ構造の説明図である。

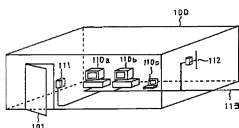
【図25】第5の実施例に係るファイル保護属性のデータ構造の説明図である。

【図26】第2の実施例に係るロック処理起動の説明図である。

【図27】第2の実施例に係る離席検出装置の設置状況の説明図である。

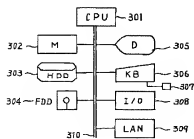
【図1】

図1



【図3】

図3



30

【図28】第3の実施例に係るロッカー一時保留機構の説明図である。

【図29】第3の実施例に係る予備制御テーブルのデータ構造の説明図である。

【図30】第3の実施例に係るアクセス制御データ整合処理起動の説明図である。

【図31】第4の実施例に係るロック画面の表示例を示す図である。

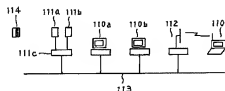
【図32】第4の実施例に係る利用者指示によるロック処理の説明図である。

【符号の説明】

400…OS、401a~b…各種タスク、401e…各種機密保護、501…ファイルアクセス要求、502…ファイルアクセス処理、503…アンロック要求、504…アンロック処理、505…ロック処理、506…データ受信、507…キー入力、600…ファイル、800…タスク制御ブロック。

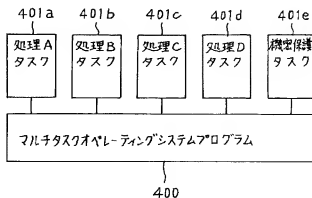
【図2】

図2



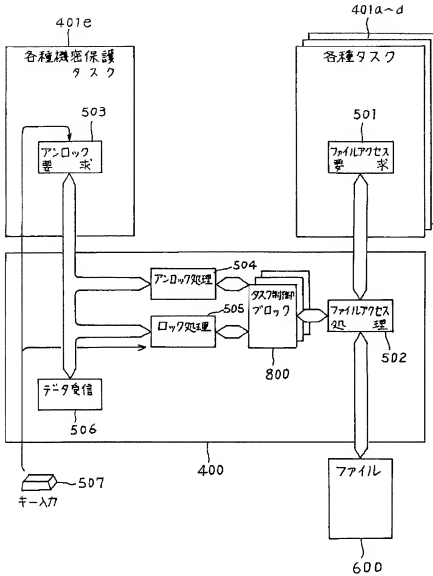
【図4】

図4



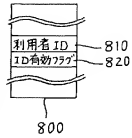
【図5】

図 5



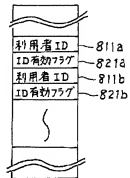
【図8】

図 8



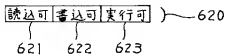
【図24】

図 24



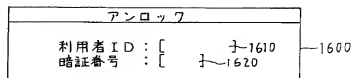
【図7】

図 7



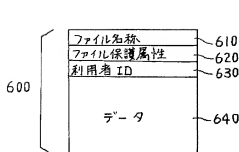
【図16】

図 16



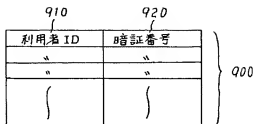
【図6】

図 6



【図9】

図 9

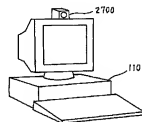
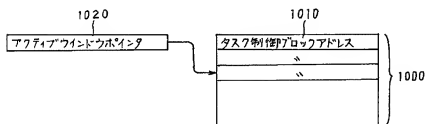


【図27】

図 27

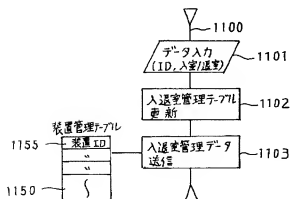
【図10】

図 10



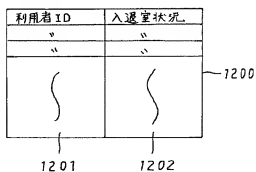
【図11】

図 11



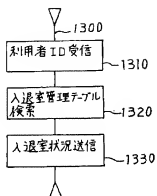
【図12】

図 12



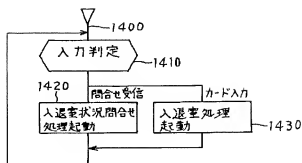
【図13】

☑ 13



【図14】

☑ 14



【図15】

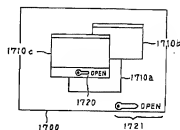
☑ 15

機密保護設定			
他人の読込:	<input type="radio"/> 可 1510	<input type="radio"/> 不可 1515	
他人の書込:	<input type="radio"/> 可 1520	<input type="radio"/> 不可 1525	
他人の実行:	<input type="radio"/> 可 1530	<input type="radio"/> 不可 1535	
利用者ID:	{ }		暗証番号: { }

1540 1550

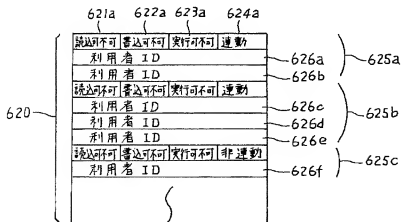
【図17】

☑ 17



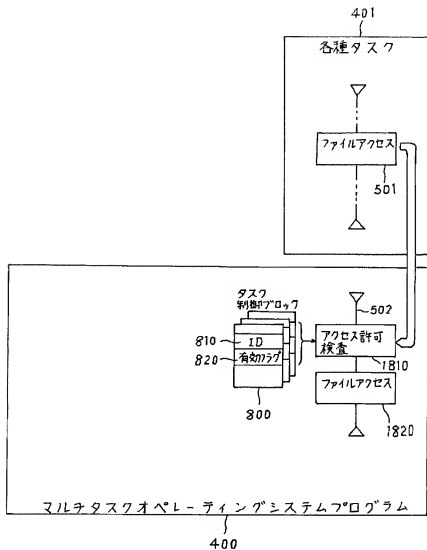
【図25】

☑ 25



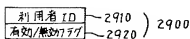
【図18】

図 18



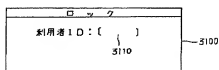
【図29】

図 29



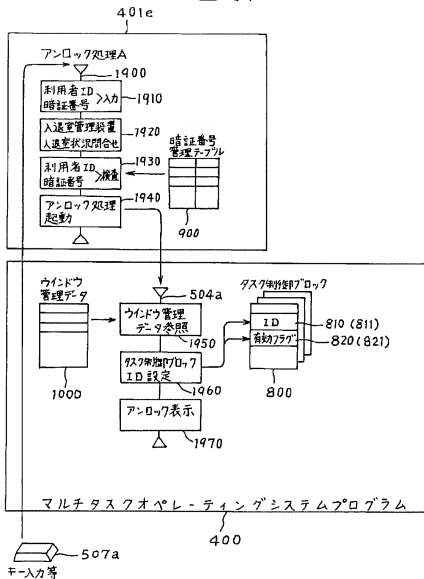
【図31】

図 31



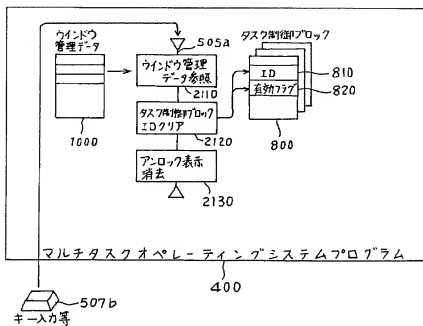
【図19】

図 19



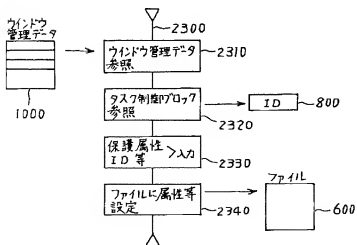
【図20】

図 20



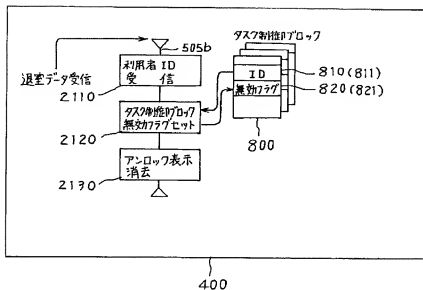
【図23】

図 23



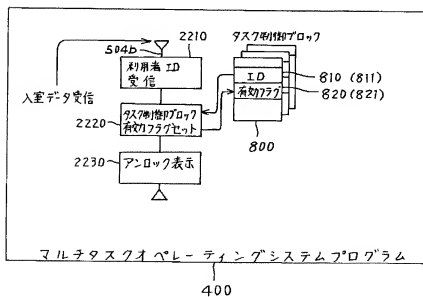
【図21】

21



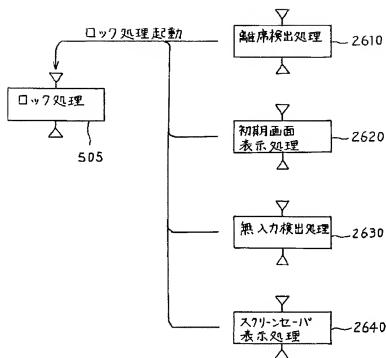
【図22】

22



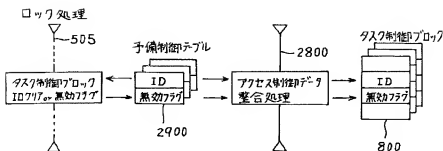
【図26】

26



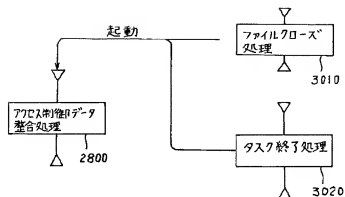
【図28】

28



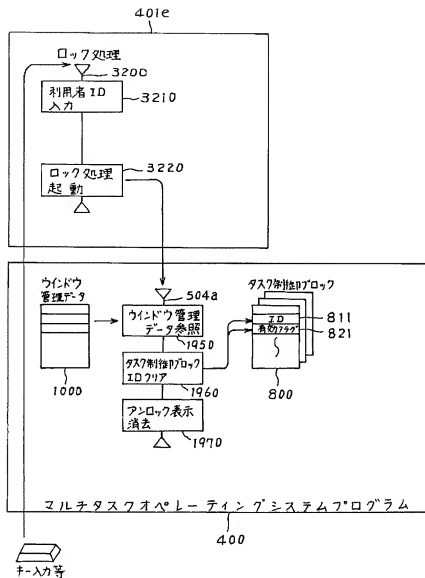
【図30】

図 30



【図32】

図 32



フロントページの続き

(72)発明者 尾崎 友哉
 横浜市戸塚区吉田町292番地株式会社日立
 製作所マイクロエレクトロニクス機器開発
 研究所内